APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/679,371	10/07/2003	Anthony C. Fascenda	62922.3	4292

21967   7590   10/25/2006

HUNTON & WILLIAMS LLP
INTELLECTUAL PROPERTY DEPARTMENT
1900 K STREET, N.W.
SUITE 1200
WASHINGTON, DC 20006-1109

EXAMINER
CHEN, SHIN HON

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 10/25/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	10/679,371	FASCENDA, ANTHONY C.
	Examiner	Art Unit	
	Shin-Hon Chen	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on _31 July 2006_.

2a) ☐ This action is **FINAL.**   2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) _1-11 and 13-28_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) _1-11 and 13-28_ is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☒ The drawing(s) filed on _07 October 2003_ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1. ☐ Certified copies of the priority documents have been received.

      2. ☐ Certified copies of the priority documents have been received in Application No. _____.

      3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1.   Claims 1-11 and 13-28 have been examined.

Claim Rejections - 35 USC § 112

2.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3.   Claims 1-11 and 19-24 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential steps, such omission amounting to a gap between the steps. See MPEP § 2172.01. The omitted steps are: the actual authentication step is not disclosed in the claims as the claims disclose a method of authentication.

Claim Rejections - 35 USC § 103

4.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5.   Claims 1-11 and 19-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pitchenik et al. U.S. Pat. No. 6397328 (hereinafter Pitchenik) in view of Hamilton et al. U.S. Pat. No. 20030097571 (hereinafter Hamilton)and further in view of Eberhard U.S. Pat. No. 5473689 (hereinafter Eberhard).

6.   As per claim 1 and 19, Pitchenik discloses a method of authenticating computing devices

on a communications network comprising the steps of: receiving a first challenge from a

computing device, wherein said first challenge comprises an encrypted first random number

(Pitchenik: column 2 lines 40-56; column 4 lines 32 – 67); obtaining a first secret cryptographic

key associated with said computing device (Pitchenik: column 2 line 40 – column 3 line 28;

column 4 lines 32 – 67); generating a second random number (Pitchenik: column 2 lines 40-56;

column 4 lines 32 – 67); decrypting said first random number with said first secret cryptographic

key (Pitchenik: column 2 lines 40-56; column 4 lines 32 – 67); encrypting said second random

number with said first secret cryptographic key (Pitchenik: column lines 40-56; column 4 lines

32 – 67); and transmitting a second challenge to said computing device, wherein said second

challenge comprises said encrypted said second random number (Pitchenik: column 2 lines 40-

56). Pitchenik discloses the host PC utilizes public key of the PSD to decrypt the encrypted

random number but Pitchenik does not explicitly disclose sending the identifier associated with

the computing device and obtaining a first secret cryptographic key associated said unique

identifier. However Hamilton discloses transmitting a unique identifier of a secure device to a

host so that a host can utilize the key associated with the secure device for authentication

purposes (Hamilton: [0015]). It would have been obvious to one having ordinary skill in the art

to inform the host about the identifier of the computing device so that host can utilize correct

security association associated with the computing device to conduct authentication process.

Therefore, it would have been obvious to one having ordinary skill in the art at the time of

applicant's invention to combine the teachings of Hamilton within the system of Pitchenik

because it allows the host to determine whether the computing device seeking authentication is

registered with host. Pitchenik does not explicitly disclose generating a second random number

where the second random number is different from the first random number. However, Eberhard

discloses both devices generate its own random number and transmit random numbers to each

other (Eberhard: column 1 line 66 – column 2 line 4 and column 3 line 45 – column 4 line 2). It

would have been obvious to one having ordinary skill in the art to generate different random

numbers when two devices try to authenticate each other. Therefore, it would have been obvious

to one having ordinary skill in the art at the time of applicant's invention to combine the

teachings of Eberhard within the combination of Pitchenik-Hamilton because using two random

numbers allows both devices to exclusively authenticate each other.

7.   As per claim 2 and 20, Pitchenik as modified discloses the method of claims 1 and 19

respectively. Pitchenik as modified further discloses wherein said unique identifier is a serial

number of a physical token installed at said computing device (Hamilton: [0015]). It would have

been obvious to one having ordinary skill in the art to utilize a tamper resistant secure device to

process authentication procedures because they ensure secure data is not leaked outside.

Therefore, it would have been obvious to one having ordinary skill in the art at the time of

applicant's invention to combine the teachings of Hamilton within combination of Pitchenik-

Hamilton-Eberhard because it allows multiple computing devices to communicate with a single

host when the host utilizes identifier of each device for authentication process.

8.   As per claim 3 and 21, Pitchenik as modified discloses the method of claims 2 and 20

respectively. Pitchenik as modified further discloses wherein said step of obtaining a first secret

cryptographic key comprises the step of retrieving a pre-stored record associated with said serial

number, wherein said record comprises said first secret cryptographic key (Hamilton: [0015]:

retrieve user key).

9.   As per claim 4 and 22, Pitchenik as modified discloses the method of claims 3 and 21

respectively. Pitchenik as modified further discloses wherein said step of obtaining a first secret

cryptographic key comprises the step of receiving a key database file comprising a number of

records, wherein each record is associated with a unique physical key token and comprises a

unique secret cryptographic key and a unique serial number (Hamilton: [0015]: the key as stored

in a database according to each serial number).

10.   As per claim 5 and 23, Pitchenik as modified discloses the method of claims 4 and 22

respectively. Pitchenik as modified further discloses wherein said unique secret cryptographic

key is created from a random number generated at initialization of said token (Hamilton: [0137]:

the user key is initialized by manufacturer to uniquely identify the security device).

11.   As per claim 6 and 24, Pitchenik as modified discloses the method of claims 1 and 19

respectively. Pitchenik as modified further discloses the method comprising the steps of:

decrypting said first challenge with a network receive cryptographic key; and encrypting said

second challenge with a network send cryptographic key (Pitchenik: column 2 line 40 – column

3 line 28; column 4 lines 32 – 67; column 3 line 60 – column 4 line 10: the key pair).

12.   As per claim 7, Pitchenik as modified discloses the method of claim 3. Pitchenik as modified further discloses wherein said step of decrypting said encrypted first random number results in a first value, and further comprising the step of disallowing said computing device to communicate with other computing devices on said network if said first value is a null value (Pitchenik: column 4 line 33 – column 5 line 4: the authentication technique can be applied to both parties).

13.   As per claim 8, Pitchenik as modified discloses the method of claim 7. Pitchenik as modified further discloses wherein allowing said computing device to communicate with other computing devices on said network if said first value is not a null value (Pitchenik: column 4 line 33 – column 5 line 4: the authentication technique can be applied to both parties).

14.   As per claim 9, Pitchenik as modified discloses the method of claim 7. Pitchenik as modified further discloses the method comprising the step of decrypting said second challenge with a network receive cryptographic key (Pitchenik: column 2 line 40 – column 3 line 28; column 4 lines 32 – 67; column 3 line 60 – column 4 line 10: the key pair).

15.   As per claim 10, Pitchenik as modified discloses the method of claim 8. Pitchenik as modified further discloses the method comprising the step of decrypting said encrypted second random number with a second secret cryptographic key (Pitchenik: column 2 line 40 – column 3 line 28; column 4 lines 32 – 67; column 3 line 60 – column 4 line 10).

16.   As per claim 11, Pitchenik as modified discloses the method of claim 10. Pitchenik as

modified further discloses wherein said second secret cryptographic key is stored within said

physical token (Pitchenik: column 2 line 40 – column 3 line 28; column 4 lines 32 – 67; column

3 line 60 – column 4 line 10).

17.   As per claim 25, Pitchenik as modified discloses the method of claim 21. Pitchenik as

modified further discloses the method comprising the steps of: receiving a third challenge from

said computing device, wherein said third challenge comprises said second random number

encrypted with a second secret cryptographic key (Pitchenik: column 2 line 34 – column 3 line

29); decrypting said encrypted second random number with said first secret cryptographic key

(Pitchenik: column 2 line 34 – column 3 line 29); and comparing said decrypted second random

number to said second random number to determine if a match exists (Pitchenik: column 2 line

34 – column 3 line 29).

18.   As per claim 26, Pitchenik as modified discloses the method of claim 25. Pitchenik as

modified further discloses wherein if a match exists between said decrypted second random

number and said second random number, allowing said computing device to communicate with

other computing device on said network, otherwise if a match does not exist, disallowing said

computing device to communicate with other computing devices on said network (Pitchenik:

column 2 line 34 – column 3 line 29).

19.   As per claim 27, Pitchenik as modified discloses the method of claim 25. Pitchenik as

modified further discloses the method comprising the step of decrypting said third challenge with

a network receive cryptographic key (Pitchenik: column 2 line 34 – column 3 line 29).

20.   As per claim 28, Pitchenik as modified discloses the method of claim 25. Pitchenik as

modified further discloses wherein said second secret cryptographic key is stored within said

physical token (Pitchenik: column 2 line 34 – column 3 line 29 and column 3 line 60 – column 4

line 10).

21.   Claims 13 and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Pitchenik in view of Hamilton and further in view of Eberhard and further in view of Shteyn

U.S. Pub. No. 20040203590 (hereinafter Shteyn).

22.   As per claim 13, Pitchenik discloses a communications system comprising: a number of

computing devices, and at least one authentication device, wherein each client device or

authentication device includes a removable unique tamper-resistant physical token comprising a

random number generator, a unique secret cryptographic key, and a unique serial number

(Pitchenik: column 2 line 40 – column 3 line 28; column 4 lines 32 – 67; column 3 line 60 –

column 4 line 10). Pitchenik does not explicitly disclose generating a second random number

where the second random number is different from the first random number. However, Eberhard

discloses both devices generate its own random number and transmit random numbers to each

other (Eberhard: column 1 line 66 – column 2 line 4 and column 3 line 45 – column 4 line 2). It

would have been obvious to one having ordinary skill in the art to generate different random

numbers when two devices try to authenticate each other. Therefore, it would have been obvious

to one having ordinary skill in the art at the time of applicant's invention to combine the

teachings of Eberhard within the system of Pitchenik because using two random numbers allows

both devices to exclusively authenticate each other. Pitchenik as modified does not explicitly

disclose wherein each tamper-resistant physical token is removable. However, Shteyn discloses

using a dongle installed via a USB to secure communications in a wireless network (Shteyn:

[0027]). It would have been obvious to one having ordinary skill in the art to store identifications

information and cryptographic key into the hardware key while authentication takes place

between a mobile terminal and an access point. Therefore, it would have been obvious to one

having ordinary skill in the art at the time of applicant's invention to combine the teachings of

Shteyn within the combination of Pitchenik-Eberhard because dongle is well known in the art for

providing security parameters within network.

23.   As per claim 17, Pitchenik as modified discloses the system of claim 13. Pitchenik as

modified further discloses wherein each tamper-resistant physical token is installed via a USB

interface. Shteyn discloses using a dongle installed via a USB to secure communications in a

wireless network (Shteyn: [0027]). It would have been obvious to one having ordinary skill in

the art to store identifications information and cryptographic key into the hardware key while

authentication takes place between a mobile terminal and an access point. Therefore, it would

have been obvious to one having ordinary skill in the art at the time of applicant's invention to

combine the teachings of Shteyn within the combination of Pitchenik-Eberhard-Kimura because

dongle is well known in the art for providing security parameters within network.

24.   Claims 14-16, and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Pitchenik in view of Eberhard and further in view of Shteyn and further in view of Kimura U.S.

Pub. No. 20010048744 (hereinafter Kimura).

25.   As per claim 14, Pitchenik as modified discloses the system of claim 13. Pitchenik as

modified does not explicitly disclose wherein each client device or authentication device further

includes a wireless communications transceiver to communicate on a wireless network.

However, it would have been obvious to one having ordinary skill in the art to apply the

authentication method to any communication environment including wireless network.

Alternatively, Kimura discloses access point authentication method and applying challenge

response and random numbers to authenticate mobile terminals within wireless LAN that

complies with IEEE 802.11 (Kimura: [0038]-[0040]). It would have been obvious to one having

ordinary skill in the art at the time of applicant's invention to apply the authentication technique

to any communication system. Therefore, it would have been obvious to one having ordinary

skill in the art at the time of applicant's invention to combine the teachings of Kimura within the

combination of Pitchenik-Eberhard because it prevents unauthorized access from mobile stations

of malicious intruders in a radio-based wireless LAN network.

26.   As per claim 15, Pitchenik as modified discloses the system of claim 14. Pitchenik as

modified further discloses wherein said wireless network is Wi-Fi network (Kimura: figure 5 and

[0004], [0035]-[0040]).

27.   As per claim 16, Pitchenik as modified discloses the system of claim 15. Pitchenik as

modified further discloses wherein said authentication device is an access point (Kimura: [0039]-

[0040] and figure 2).

28.   As per claim 18, Pitchenik as modified discloses the system of claim 16. Pitchenik as

modified further discloses wherein said access point includes a database file comprising said

serial numbers and secret cryptographic keys associated with said tokens (Pitchenik: column 3

line 60 – column 4 line 10; Kimura: [0004], [0035]-[0040]).

Response to Arguments

29.   Applicant's arguments with respect to claims 1-11 and 13-28 have been considered but

are moot in view of the new ground(s) of rejection.

30.   In view of the Appeal Brief filed on 7/31/06, PROSECUTION IS HEREBY

REOPENED. A new ground of rejection is set forth above.

        To avoid abandonment of the application, appellant must exercise one of the following

two options:

        (1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37

CFR 1.113 (if this Office action is final); or,

        (2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an

appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee

can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have

been increased since they were previously paid, then appellant must pay the difference between

the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing

below:

Conclusion

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Shin-Hon Chen whose telephone number is (571) 272-3789. The

examiner can normally be reached on Monday through Friday 8:30am to 5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the

organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would

like assistance from a USPTO Customer Service Representative or access to the automated

information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Shin-Hon Chen
Examiner
Art Unit 2131

SC

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100